Janusz BARTA
Ryszard MARKIEWICZ

PRAWO DO PRYWATNOŚCI W SPOŁECZEŃSTWIE INFORMATYCZNYM

> *Globalne sieci komputerowe [...] przyniosły ze sobą zwiększone niebezpieczeństwo ingerencji w prawo do prywatności i – spokrewnione z nim – prawo do tajemnicy korespondencji. Istnieje obawa naruszenia tej podstawowej, osadzonej w prawach osobistych [...], kompetencji przynależnej człowiekowi, która pozwala mu samodzielnie decydować o tym, które informacje na jego temat [...] zostaną podane do wiadomości publicznej względnie będą gromadzone bez wiedzy zainteresowanego.*

1. Kwestia poszanowania prywatności jednostki nie jest bynajmniej dla prawników zagadnieniem nowym. Jak się powszechnie przyjmuje, pojęcie i koncepcja „right to privacy" ma już swoją ponad stuletnią historię[1]. Można nie bez podstaw twierdzić, iż w tym okresie systematycznie rosło znaczenie tej problematyki, która coraz mocniej wrastała w katalog podstawowych praw i wolności człowieka, chronionych w poszczególnych krajach przez przepisy rangi konstytucyjnej oraz przez akty międzynarodowe. Do podstawowych norm w tym zakresie należy niewątpliwie artykuł 8. Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności z 1950 roku[2]. Stwierdza on:

„1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.

2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób"[3].

---

[1] Geneza tego prawa, w aspekcie prawa pozytywnego, wiązana jest najczęściej z amerykańskimi prawnikami S. D. Warrenem i L. D. Brandeisem, autorami artykułu zatytułowanego *Right to Privacy*, opublikowanego w 1890 r. w „Harvard Law Review".

[2] Na temat koncepcji i ochrony prawa do prywatności w świetle ustawodawstw krajowych, a zwłaszcza konwencji międzynarodowych, patrz w literaturze polskiej m.in.: L. K a ń s k i, *Prawo do prywatności, nienaruszalności mieszkania i tajemnicy korespondencji*, w: *Prawa człowieka, model prawny*, Wrocław – Warszawa – Kraków 1991, s. 317n.

[3] Jak łatwo zauważyć, mamy tu do czynienia z uregulowaniem znacznie bardziej rozbudowanym niż to, które znajdujemy w podobnie brzmiących postanowieniach Powszechnej Deklaracji Praw Człowieka oraz Międzynarodowego Paktu Praw Obywatelskich i Politycznych: „Nikt nie

Z zacytowanego przepisu, zaznaczmy, wynikają nie tylko pewne gwarancje ochronne, ale też pozytywne obowiązki adresowane do państw członkowskich konwencji co do troski o poszanowanie życia prywatnego i rodzinnego, łącznie ze stosunkami międzyludzkimi[4].

Długa historia prawa do prywatności nie oznacza bynajmniej, że mamy tu do czynienia z instytucją prawną o wyraźnie określonej treści i zakresie stosowania. I nie chodzi tylko o rozmaite prawnicze konstrukcje, które prawo do prywatności ujmują węziej lub szerzej (rozciągając je na przykład na prawo do wolności przekonań, wolności słowa, wolności zrzeszania się). Zmiany wynikają też, lub przede wszystkim, z przeobrażeń warunków społecznych, w których żyje i pracuje człowiek, co łączy się nierozerwalnie z rozwojem techniki, a także ze zmianą poglądów i oczekiwań względem systemu prawnego[5]. Wspomniane prawo, pomyślane i funkcjonujące pierwotnie jako instrument pozwalający bronić się przed wścibską, natarczywą prasą, ma obecnie do spełnienia znacznie szersze zadania. Szczególne wyzwania stawiane są przez kształtujący się obecnie nowy model „społeczeństwa informatycznego". Określenie to, które w ostatnim okresie zrobiło ogromną karierę, nie ma jednej, przyjętej przez wszystkich definicji. Próba jej sformułowania nie jest zresztą naszym celem. W artykule tym poprzestaniemy na wskazaniu jednej istotnej cechy takiego społeczeństwa i pewnych płynących z niej konsekwencji. Otóż chodzi tu o społeczeństwo, w którego funkcjonowaniu ważną rolę odgrywa technika informatyczna. Być może już niedługo będzie można nawet powiedzieć, iż chodzi o społeczeństwo zdominowane przez technikę informatyczną.

Technika ta, rozwijająca się bardzo szybko, oferuje coraz więcej różnorakich możliwości. I znów wskażmy tylko niektóre jej funkcje czy właściwości. Użytkownikowi zostały zaoferowane:

a) niezwykle wielkie zasoby informacji (nieporównywalne z tymi, które mógł pozyskać członek „tradycyjnego" społeczeństwa, korzystający z prasy, książek, wykładów itp.);

b) łatwe, efektywne i „wygodne" formy dostępu do informacji;

c) nowe sposoby przekazywania informacji między dowolnymi punktami na ziemi; mówi się obrazowo o „informacyjnych autostradach", na których panuje wielki ruch, po których w wielu kierunkach mkną z olbrzymią szybkością sprowadzone do cyfrowego zapisu najrozmaitsze materiały (pisemne, graficzne, obrazowe, muzyczne itp.);

może być poddany arbitralnemu ingerowaniu w jego życie prywatne, rodzinne, domowe lub korespondencję ani też atakom na jego honor i dobre imię. Każdy człowiek ma prawo do ochrony prawnej przeciwko takim ingerencjom i atakom".

[4] Por. M. A. N o w i c k i, *Europejska Konwencja Praw Człowieka*; *wybór orzecznictwa*, Warszawa 1998, s. 266, 270.

[5] I tak na przykład zaczęto przyjmować, iż prawo do prywatności nie sprowadza się do „prywatności jednostki", lecz obejmuje także sferę osób najbliższych, rodziny.

d) nowe sposoby porozumiewania się z innym członkami społeczeństwa, wymiany poglądów, dyskusji;

e) nowe sposoby prowadzenia działalności komercyjnej, sprzedawania towarów i usług, dokonywania płatności.

Fascynacji tymi zjawiskami towarzyszą jednak także pewne obawy. Pojawiają się trudności poruszania się w olbrzymim zalewie informacji, często informacji o trudnym do ustalenia pochodzeniu i wiarygodności. Wskazuje się na to, że kontakty między ludźmi stają się coraz bardziej anonimowe, zostają zerwane lub słabną tradycyjne więzi międzyludzkie, wzrasta poczucie alienacji jednostki. Można by powiedzieć, iż – paradoksalnie – sieci komputerowe stwarzają dobre warunki do realizacji prawa do prywatności, które – jak wyjaśniają niektórzy – wyraża się w „prowadzeniu egzystencji samotnej i anonimowej".

2. Tymczasem starając się wychwycić rozmaite ujemne konsekwencje związane z postępem techniki komputerowej, a zwłaszcza z ekspansją Internetu, bardzo często zwraca się uwagę właśnie na nowe przypadki zagrożenia dla prywatności człowieka[6]. Im dalej w życie społeczne wkraczają sieci komputerowe, im bliższe staje się urzeczywistnienie tego, co, z pewnym uproszczeniem, określa się mianem społeczeństwa informatycznego, tym bardziej rośnie skala tego niebezpieczeństwa. Zdaniem niektórych właśnie ochrona praw osobistych, zwłaszcza prawa do prywatności, a ściślej, brak w tej materii powszechnie aprobowanych uregulowań uwzględniających nowe zjawiska społeczne związane z ekspansją globalnych sieci informatycznych, stanowić może podstawową barierę dalszego wykorzystania tych sieci w obrocie prawnym i handlowym. Wyrażana jest też opinia, iż jest to obecnie bodajże najważniejsze zagadnienie związane z wykorzystaniem Internetu [7].

Dysputom i rozważaniom prawników na temat „Privacy in Cyberspace" towarzyszy przy tym poczucie zagrożenia wśród samych użytkowników globalnych sieci. Potwierdzają to wyniki badań prowadzonych zarówno w Europie, jak i w USA. Użytkownicy Internetu coraz wyraźniej dostrzegają, iż „włączenie się przez nich do ruchu" na międzynarodowych autostradach informatycznych niesie ze sobą ryzyko ujawnienia i utraty kontroli nad cyrkulacją oraz wyko-

[6] Przyjmujemy na potrzeby tego artykułu definicję prywatności zaproponowaną przez A. Kopffa: „to wszystko, co ze względu na uzasadnione odosobnienie się jednostki od ogółu społeczeństwa służy jej do rozwoju fizycznej i psychicznej osobowości oraz zachowania osiągniętej pozycji społecznej". Podzielamy przy tym pogląd o istnieniu „ponad" sferą prywatności sfery intymności, która obejmuje ten zakres faktów dotyczących jednostki i jej przeżyć, który w zasadzie nie jest przez nią ujawniany nawet osobom najbliższym i którego odsłonięcie przed kimkolwiek wywołuje zawsze uczucie wstydu, zakłopotania i udręki. Por. A. K o p f f, *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, „Studia Cywilistyczne" t. 20, s. 32n., 37.

[7] Por. w tej kwestii Surfer Beware: Personal Privacy and the Internet, June 1997, Electronic Privacy Information Center, Washington, DC, http://www.epic.org/reports/surfer-beware.html.

rzystaniem różnych danych osobowych na ich temat, w tym też ryzyko niedostrzegalnego wkraczania w sferę ich prywatności, inwigilacji prowadzonej przy użyciu nowoczesnej technologii informatycznej[8].

W jakich okolicznościach najczęściej pojawia się wspomniane ryzyko? W czym tkwi jego źródło? Spróbujmy wskazać na niektóre charakterystyczne przypadki.

I tak, już na wstępie, nasuwa się hipoteza, iż równolegle do wzrostu ilości dostępnych informacji, co dzieje się za sprawą Internetu, wzrasta też możliwość oraz zakres pojawienia się informacji dotykających sfery prywatności. Poza tym trzeba zauważyć, że sam Internet stanowi szczególny, rozwinięty na wielką skalę, środek masowego komunikowania, środek porozumiewania się, platformę wymiany poglądów i dyskusji. Sieci komputerowe tworzą swoisty wirtualny plac, gdzie spotykają się, przemawiają i rozmawiają wielkie rzesze ludzi (dysponenci podłączonych do sieci komputerów). Z natury rzeczy, niejako z istoty swych funkcji, tego rodzaju środki i sytuacje niosą z sobą niebezpieczeństwo udostępniania przy okazji, lub nawet w sposób zamierzony, informacji, które należą do sfery prywatności. Dostrzec to można obserwując powstawanie i rozwój tradycyjnych środków masowego komunikowania, takich jak prasa, radio, telewizja.

Równocześnie skala owych zagrożeń wzrasta przez to, iż sieć Internetu stała się nowym medium przekazu dla owych tradycyjnych form prasowych. Tak więc w Internecie już dziś znajdujemy „internetowe wydania" dzienników i czasopism. Bywają one bądź wiernym powtórzeniem („kalką") edycji drukowanych, bądź swoistą ich mutacją. Takie internetowe wydania otwierają przy tym rozległe możliwości „odchodzenia w bok" do innych dostępnych w Internecie zbiorów informacji, do innych stron www., przy wykorzystaniu systemu odesłań (hyperlinks i links). Możemy zatem stanąć wobec sytuacji, w której wprawdzie „w tekście zasadniczym", odpowiadającym temu, co znalazło się w edycji drukowanej, nie znajdują się żadne materiały wkraczające w sferę prywatności jednostki, natomiast pojawią się one w zbiorach, do których „odwiedzenia" namawiają nas wspomniane odesłania wprowadzone do tekstu zasadniczego.

Mówiąc o tradycyjnych środkach masowego komunikowania znajdujących się w Internecie należy pamiętać, iż z tej drogi rozpowszechniania korzysta nie tylko prasa drukowana, ale zainteresowani są nią także nadawcy radiowi i telewizyjni. Wprowadzenie programów radiowych i telewizyjnych do sieci komputerowych staje się już rzeczywistością. W szybkim tempie zbliżamy się do sytuacji, w której komputer, wraz z odpowiednim wyposażeniem, zastępować

[8] Por. m.in.: C. de T e r w a n g n e, S. L o u v e a u x, *Data Protection and Online Network*, „Multimedia und Recht" 1998, nr 9, s. 451n.

będzie wiele dotychczasowych środków przekazu informacji (odbiornik radiowy i telewizyjny, telefon, fax).

Dziś trudno sobie jeszcze wyobrazić wszystkie konsekwencje tego, co określa się mianem konwergencji rozmaitych sieci telekomunikacyjnych. Odnosi się to również do konsekwencji w sferze ochrony praw osobistych. Nie ulega jednak wątpliwości, iż wśród wielu problemów także problem poszanowania podstawowych praw i wolności człowieka, między innymi prawa do prywatności, wymagać będzie w tym kontekście ponownej analizy.

3. Niebezpieczeństwa wkraczania w prywatność człowieka w związku z posługiwaniem się Internetem nie wynikają jednak tylko, lub nawet przede wszystkim, z funkcji, jakie on spełnia. Poważne obawy wywołują te istniejące możliwości techniczne (informatyczne), które pozwalają prowadzić różnego rodzaju „nasłuch" i wpływać na przepływ informacji. Chodzi, po pierwsze, o to, że zachowanie się użytkowników w sieci może być przez osoby trzecie w sposób nieuchwytny obserwowane. Za pomocą specjalnych programów (tzw. „packet sniffers") wyszukiwane mogą być przepływające w sieci komunikaty określonego rodzaju, na przykład wybierane według słów kluczowych lub według danych z karty kredytowej. Nie nastręcza dziś większych trudności ustalenie, czym dany użytkownik Internetu się interesuje, jakie odwiedzał strony, w jakich grupach dyskusyjnych uczestniczył, jakie „ściągał" informacje, jakich dokonywał transakcji i operacji finansowych za pośrednictwem Internetu, z kim prowadził elektroniczną korespondencję. Krąg wyszukiwanych informacji można zacieśniać jeszcze bardziej i badać na przykład, jakie poglądy wyrażał w dyskusjach prowadzonych przy wykorzystaniu Internetu[9].

Powody zainteresowania takimi informacjami mogą być rozmaite i nie sprowadzają się bynajmniej do czystej ciekawości. Jeśli nawet pominiemy interes występujący w przypadku policji czy służb specjalnych, to i tak grupę zainteresowanych tworzyć mogą między innymi aktualni albo potencjalni pracodawcy danej osoby, instytucje finansowe (banki, kredytodawcy), czy wreszcie producenci (dostarczyciele) towarów i usług oraz firmy zajmujące się marketingiem, badaniami rynku lub reklamą. Zebrane dane pozwalają bowiem zorientować się, jakie są poglądy określonej osoby w różnych kwestiach, jaka jest jej sytuacja osobista, jakie są jej zwyczaje, zainteresowania i preferencje, w tym także handlowe. Posługując się większą ilością danych można pokusić się o konstruowanie tak zwanych profilów osobowościowych. Nie trzeba przy tym dodawać, że tego rodzaju wiadomości mogą mieć wymierną, i to wcale niemałą, wartość majątkową.

[9] Można oczywiście dyskutować, czy w tego rodzaju przypadkach należy stwierdzić naruszenie prawa do prywatności, czy też raczej opisane przypadki należy kwalifikować jako naruszenie tajemnicy korespondencji, przy nadaniu pojęciu „korespondencja" szerokiego znaczenia.

Prowadzenie w ramach Internetu różnorakiej i ożywionej działalności wywołało również zjawisko nowych „wymiarów prywatności": mamy na myśli te aspekty, które wiążą się z identyfikowaniem osób komunikujących się za pośrednictwem Internetu. Jak można zauważyć, dane, takie jak imię, nazwisko osoby czy miejsce jej zamieszkania, są uzupełniane lub zastępowane przez wybraną sekwencję znaków (liter) określanych jako adres internetowy lub adres e-mail. Powstał problem ujmowania takich danych w kategorii dóbr osobistych i czynienia z nich przedmiotu ochrony, podobnie jak to ma miejsce w przypadku prawa do nazwiska.

Wreszcie wydaje się, iż nie sposób pominąć jeszcze jednej okoliczności przy rozważaniu niebezpieczeństw naruszania prywatności w sieci Internetu. Mamy na myśli – ujmując to skrótowo – swego rodzaju „poczucie bezkarności". Wynika ono, z jednej strony, z nie wyjaśnionej pod wieloma względami sytuacji prawnej (właściwych norm prawnych, zasad odpowiedzialności), jeśli chodzi o zdarzenia mające miejsce w Internecie. Z drugiej strony takiemu nastawieniu sprzyja anonimowość wielu działań podejmowanych w otwartych i rozległych sieciach komputerowych, z czym wiąże się trudność dochodzenia ochrony. Z całą wyrazistością uwidacznia się pytanie: kto odpowiada za zniesławiające, godzące w dobra osobiste wypowiedzi i materiały pojawiające się w sieciach?

Nie dziwi zatem, że w opinii niektórych osób Internet jawi się jako obszar anarchii lub jako teren niejako wyłączony spod działania prawa. O ile w pierwszym poglądzie zawarta jest ocena negatywna, o tyle wyjęcie Internetu spod działania prawa traktuje się niejednokrotnie jako zjawisko w pewnej mierze pozytywne, zasługujące na obronę w imię pełnej i nieskrępowanej realizacji swobody wypowiedzi. Próby wprowadzenia prawnej regulacji na tym polu traktowane są jako zamach na wspomniane swobody; nierzadko szermuje się sugestywnymi hasłami odwołującymi się do niebezpieczeństwa wprowadzenia w Internecie cenzury.

Z drugiej strony podejmowanie zagrażających prywatności kroków, które mają na celu kontrolowanie tego, co „przepływa" w Internecie, usprawiedliwiane bywa między innymi racjami wyższymi, obroną bezpieczeństwa publicznego, walką z przestępczością. I tak kontrolowanie płatności dokonywanych za pomocą kart przez sieci komputerowe wyjaśnia się tym, iż właśnie tego rodzaju sieci dały szansę łatwego „prania brudnych pieniędzy". A więc – konkludują niektórzy – jeśli chce się walczyć z różnymi postaciami przestępczości komputerowej, należy zgodzić się na monitorowanie przepływu danych. Czasami pojawia się też myśl, z którą trudno się zgodzić, iż w przypadku udostępnienia swych danych „przy okazji" transakcji dokonywanej w sieciach udzielana jest domniemana zgoda osoby, która jest stroną takiej transakcji (konsumenta), na magazynowanie tych danych, ich opracowywanie przez kontrahenta dla potrzeb własnych.

Jak zatem można zauważyć, globalne sieci komputerowe, a wśród nich najbardziej znana sieć Internet, przyniosły ze sobą zwiększone niebezpieczeństwo ingerencji w prawa osobiste człowieka, a w szczególności w prawo do prywatności i – spokrewnione z nim – prawo do tajemnicy korespondencji. Istnieje obawa naruszenia przede wszystkim tej podstawowej, osadzonej w prawach osobistych (czy wprost: w prawie do prywatności), kompetencji przynależnej człowiekowi, która pozwala mu samodzielnie decydować o tym, które informacje na jego temat (być może z wyjątkiem jedynie tych, które są powszechnie dostępne i mają całkowicie „neutralny" charakter) zostaną podane do wiadomości publicznej względnie będą gromadzone bez wiedzy zainteresowanego.

To stwierdzenie prowadzi nas w obszar problemów prawnych, które ostatnio zyskały na znaczeniu, tworząc właściwie autonomiczny przedmiot regulacji, aczkolwiek ściśle powiązany z prawem do prywatności. Mamy na myśli problematykę ochrony danych osobowych.

Dostrzegł ją w Polsce w jednym ze swych orzeczeń Trybunał Konstytucyjny (K 21/96, 225), wydanym jeszcze – co trzeba uwzględnić – przed uchwaleniem ustawy o ochronie danych osobowych, a także obowiązującej dziś Konstytucji RP. Uznał mianowicie, że gwarancja prawa do prywatności jest niejako immanentnym elementem demokratycznego państwa prawnego, i stwierdził, że prawo do prywatności oznacza między innymi „prawo do zachowania w tajemnicy informacji o swoim życiu prywatnym". Wiąże się z tym – według Trybunału – konieczność ochrony tajemnicy danych dotyczących sytuacji majątkowej obywatela, w tym jego transakcji dokonywanych za pośrednictwem banków.

4. Zastanawiając się nad kwestią ochrony prywatności z perspektywy zjawisk, które dotyczą zbierania i wykorzystywania danych osobowych, można by sądzić, iż prawne aspekty tego zagadnienia nie są zależne od uwarunkowań technicznych. Przecież w równej mierze niedozwolone może (czy powinno) być gromadzenie danych osobowych na czyjś temat, a potem ich udostępnianie, przy posługiwaniu się papierowymi kartotekami, co z użyciem nośników elektronicznych. Istotne są nie techniczne sposoby, lecz raczej to, jakie dane i do jakich celów są wykorzystywane. Takie stwierdzenia można uznać za trafne, ale niepełne. Nie można zapominać, że technika komputerowa pozwala w ułamkach sekund, a przy tym stosunkowo tanio i wyczerpująco, wyszukiwać według podanych kryteriów w olbrzymich zasobach interesujące dane, pozwala zestawiać i łączyć różne zbiory tworzone z różnym przeznaczeniem, a niekiedy daleko od siebie zlokalizowane. Wszystko to stwarza zupełnie „nową jakość", jeśli chodzi o eksploatację danych osobowych, a co za tym idzie – także o ich ochronę. Coraz powszechniejsze korzystanie z techniki komputerowej oraz jej gwałtowny rozwój stanowiły niewątpliwie silny impuls, który przyczynił się do wprowadzenia w życie na forum krajowym i międzynarodowym szczególnych uregulowań dotyczących ochrony danych osobowych. Można też nie bez pod-

staw przyjąć, iż właśnie w kontekście nowoczesnej techniki informatycznej omawiana ochrona zaczęła „awansować", zyskując w niektórych krajach gwarancje konstytucyjne.

Znalazło to w pewnej mierze odbicie także w polskim systemie prawa. Obowiązująca Konstytucja RP stwierdza między innymi, że:

a) „Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby" (art. 51, ust. 1);

b) „Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa" (art. 51, ust. 3);

c) „Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą" (art. 51., ust. 4).

Przetwarzania danych osobowych, w pełnym tego słowa znaczeniu, dotyczy tylko artykułu 51., ustęp 2. Konstytucji. Postanowienie to przewiduje, że: „W ł a d z e p u b l i c z n e [podkr. J.B. i R.M.] nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym". Tak więc nie mieści się w przedmiotowym zakresie tego przepisu takie pozyskiwanie, a także przetwarzanie informacji o obywatelach, które dokonywane jest przez instytucje niepubliczne, osoby prawne i fizyczne; można powiedzieć – nie stanowi ono naruszenia przepisów konstytucyjnych, znajduje się poza ramami konstytucyjnych wolności i praw osobistych. Tak samo należy ocenić udostępnianie i obrót danymi osobowymi przez podmioty niepubliczne[10].

Wspomnianej wyżej regulacji zamieszczonej w Konstytucji towarzyszy następująca zapowiedź (wyrażona w art. 51, ust. 5): „Zasady i tryb gromadzenia i udostępniania informacji określa ustawa". Za spełnienie tej zapowiedzi uznać trzeba wydanie ustawy z dnia 28 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. nr 133, poz. 883)[11]. Formułuje ona na wstępie – w artykule pierwszym – dwa główne założenia :

a) „Każdy ma prawo do ochrony dotyczących go danych osobowych";

b) „Przetwarzanie danych osobowych[12] może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą".

---

[10] Takie ujęcie jednak nie przeszkadza temu, iż również w tych przypadkach konstytucja gwarantuje indywidualne uprawnienia wymienione wyżej w punkcie a) – prawo do zachowania w poufności danych osobowych i w punkcie c) – prawo do sprostowania lub usunięcia informacji zebranych „wadliwie" lub o „wadliwej" treści. Ale już prawo dostępu do zbioru danych zostało ograniczone do tych przypadków, gdy w grę wchodzą zbiory lub dokumenty urzędowe.

[11] Określana skrótowo : „u.o.d.o.".

[12] „Przetwarzaniem danych – zgodnie z definicją zamieszczoną w art. 7, pkt 2. u.o.d.o. – są jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, prze-

W świetle tych założeń wydaje się usprawiedliwione przyjęcie tezy, iż de lege lata zasadą jest zakaz przetwarzania jakichkolwiek danych osobowych bez zgody ze strony zainteresowanego; „legalizacja" wymaga wskazania dobra (powszechnego lub indywidualnego), które by przemawiało za prowadzeniem takich działań. Chodzi przede wszystkim o takie sytuacje, gdy jest to niezbędne: a) w celu ochrony żywotnych interesów osoby, której dane dotyczą, a nie jest możliwe uzyskanie zgody osoby zainteresowanej[13]; b) w celu wykonywania określonych prawem zadań realizowanych dla dobra publicznego; c) w celu wypełniania usprawiedliwionych zadań administratorów danych (którzy przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych), o ile – jak zastrzega ustawa – przetwarzanie danych nie narusza praw i wolności tej osoby, której dane dotyczą[14]. Jeżeli chodzi natomiast o udostępnianie innej osobie takich danych, które zostały już zgromadzone przez administratora zbioru, to jest to na ogół dozwolone wówczas, gdy osoba ta w sposób wiarygodny uzasadni potrzebę posiadania tych danych. Dodane jest jednak zastrzeżenie: „a ich udostępnianie nie naruszy praw i wolności osób, których dane te dotyczą".

Takie ujęcie jest jednak tylko pozornie rygorystyczne. Prawie zawsze będzie można wskazać na czyjeś dobro, w imię którego takie przetwarzanie może być dokonywane. Zauważmy, że może to być jakiekolwiek dobro, interes, a więc także majątkowy[15]. Punkt ciężkości przesuwa się na ustalenie, czy przetwarzanie danych nie narusza praw i wolności osób, których te dane dotyczą.

Od razu nasuwa się pytanie: jakie prawa i wolności ustawodawca ma tu na myśli? Z pewnością nie chodzi o „prawo do ochrony danych osobowych", o prawo decydowania o przetwarzaniu informacji dotyczących danej osoby, lecz właśnie o przesłankę „legalizującą" wkroczenie w sferę tych praw.

---

chowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych". Ustawodawca polski nie przyjął znanego niektórym zagranicznym porządkom prawnym rozwiązania, które poza zakresem pojęcia „przetwarzanie danych" stawia dwie odrębne kategorie: „zbieranie danych" i „wykorzystywanie danych", czego konsekwencją jest odrębne traktowanie ograniczeń w sferze przetwarzania i w sferze wykorzystywania danych.

[13] Legalizacja w oparciu o tę okoliczność traci znaczenie z chwilą, gdy uzyskanie zgody staje się możliwe.

[14] Dodatkowe wymogi stawiane są wówczas, gdy przetwarzanie danych następuje w innym celu niż ten, dla którego były zebrane. Ustawa nakazuje, aby takie przetwarzanie: a) nie naruszało praw i wolności osób, których dotyczą, oraz b) następowało w celach badań naukowych, dydaktycznych, historycznych lub statystycznych.

[15] Za taką interpretacją przemawia też art. 3, ust. 2., który stanowi między innymi o przetwarzaniu danych w związku z działalnością zarobkową czy zawodową. Dopiero gdybyśmy uznali, iż w zacytowanym przepisie chodzi o „dobra prawem chronione", pole dopuszczalnego przetwarzania danych uległoby istotnemu ograniczeniu.

Zwrot, jakim się posłużył ustawodawca, a mianowicie mówienie o „prawach i wolnościach osoby", wywołuje ścisłe skojarzenia z materią konstytucyjną. Jest to zwrot używany w normach konstytucyjnych, a nawet w tytułach części Konstytucji (Konstytucja wyróżnia „wolności i prawa" osobiste, polityczne, ekonomiczne, socjalne i kulturalne). Można zatem bronić zdania, iż warunkiem dopuszczalności przetwarzania danych jest to, aby owo przetwarzanie nie naruszało żadnego z praw czy wolności konstytucyjnych. Analiza odpowiednich postanowień Konstytucji prowadzi do wniosku, iż może tu chodzić o nienaruszanie:

a) „prawa do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym" (art. 47 Konstytucji RP);

b) „prawa do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą" (art. 51, ust. 4).

W grę może wchodzić jeszcze:

c) „wolność i ochrona tajemnicy komunikowania się" (art. 49).

W tym kontekście niewątpliwie centralnym zagadnieniem pozostaje kwestia poszanowania prawa do prywatności. Rysuje się tu jednak niebezpieczeństwo popadnięcia w swego rodzaju wewnętrzną sprzeczność. Mielibyśmy bowiem do czynienia z regulacją, która zezwala na przetwarzanie danych osobowych, a więc z istoty swej zezwala także na niejednokrotne wkraczanie w prawo do prywatności, jednakże równocześnie zastrzega, iż zezwolenie to nie może naruszać prawa do prywatności. Jeżeli przepis ten ma zachować jakąś racjonalną treść, należy go interpretować w ten sposób – za czym się opowiadamy – że wspomniane zastrzeżenie nie obejmuje „tego segmentu prawa do prywatności", który odnosi się do swobody dysponowania własnymi danymi osobowymi.

Sytuacja nie zmieni się wiele, gdy odrzucimy tezę, iż omawiany przepis ustawy odwołuje się do praw i wolności uwzględnionych w Konstytucji. Poszukując dodatkowych, „pozakonstytucyjnych" praw i wolności, które nie powinny być naruszane przy przetwarzaniu danych osobowych, dodać można do prawa do prywatności i prawa do dobrego imienia ewentualnie jeszcze prawo do wizerunku czy prawo kultu pamięci osoby zmarłej. Wszystkie te dalsze prawa odgrywają jednak, jak można przyjąć, w stosunku do prawa do prywatności znaczenie drugorzędne[16].

[16] Dodajmy, iż w niektórych zagranicznych ustawodawstwach przetwarzania danych osobowych przez podmioty niepubliczne nie uzależnia się od nienaruszania ogólnikowo ujętych praw i wolności, lecz stanowi się wprost i wyłącznie o poszanowaniu życia prywatnego i rodzinnego (tak np. ustawa austriacka). Spotkać jednak można też przykłady klauzul bardziej ogólnych, jak to ma miejsce w ustawie francuskiej, która zaznacza, iż przetwarzanie danych musi następować przy poszanowaniu „życia prywatnego oraz wolności indywidualnych i publicznych".

5. Przedstawione rozważania na temat ustawy o ochronie danych osobowych kierują uwagę na określenie jej funkcji. Nie bez racji można bronić poglądu, iż główne zadanie tego aktu prawnego polega nie na tym, aby z każdej pojedynczej danej osobowej czynić dobro prawne, lecz aby stworzyć taki dający się realizować model ochrony, który by pozwalał i nakazywał badać przy każdym przetwarzaniu danych, czy dla takiego działania istnieje „słuszny interes" po stronie tego, który je prowadzi, i czy nie zostaną przy tym nieproporcjonalnie naruszone zasługujące na ochronę interesy osób zainteresowanych (tych, których dane dotyczą). Taka koncepcja, jak łatwo zauważyć, oparta jest na metodologicznym założeniu „oceniania i wyważania interesów". W efekcie – jak piszą niektórzy – rozstrzyganie o dopuszczalności przetwarzania danych wymaga trzystopniowej procedury: a) oznaczenia interesów, b) oceny interesów, c) wyważania wzajemnie konkurencyjnych interesów. Ponieważ pojedyncze dane osobowe nie mają statusu chronionego dobra prawnego, przeto nie można każdego ich przetwarzania pojmować jako naruszenie „zasługujących na ochronę interesów". Natomiast gdy uznamy, iż do naruszenia takiego interesu doszło, należałoby badać i porównywać konkurencyjny interes występujący po stronie tych, którzy dokonują, i tych, którzy korzystają z przetwarzania danych.

Kończąc tę część wywodów można dodać, iż tło, a w pewnej mierze i źródło podanych wyżej w uproszczeniu koncepcji uregulowania dopuszczalności przetwarzania danych osobowych stanowią do pewnego stopnia poglądy filozoficzno-socjologiczne. Mają one wpływ na to, czy na człowieka patrzy się bardziej pod kątem jego udziału w życiu społecznym, widząc w nim członka zbiorowości (i wówczas łatwiej jest akceptować dalej idące swobody w sferze przetwarzania danych osobowych), czy też w większym stopniu eksponuje się indywidualność osoby ludzkiej, a nawet jej intymność (i wówczas jesteśmy skłonni stworzyć bardziej surowe ograniczenia w zbieraniu i wykorzystywaniu takich danych)[17].

6. Decydując o mniejszym lub większym ograniczeniu swobody przetwarzania danych należy uwzględniać innego rodzaju, poniekąd konkurencyjne, swobody, w obszar których równocześnie wkraczamy. Mamy na myśli swobodę dostępu i przepływu informacji[18]; niekiedy w literaturze zagranicznej mówi się nawet o istnieniu prawa jednostki do zbierania i przetwarzania danych. Nie jest zatem pozbawione racji stwierdzenie, iż regulacje prawne dotyczące ochrony danych osobowych, a także przetwarzania takich danych, stanowią swoistą

[17] Por. H. E h m a n n, *Zur Zweckbindung privater Datennutzung*, „Recht der Datenverarbeitung" 1988, nr 4, s. 172.

[18] Przypomnijmy w tym miejscu, iż obowiązująca Konstytucja RP zapewnia każdemu wolność pozyskiwania i rozpowszechniania informacji (art. 54, ust. 1). Powstaje jednak wątpliwość, na ile wolność pozyskiwania informacji można traktować jako podstawę żądania dostępu do informacji.

wypadkową między szeroko unormowanym prawem do prywatności osób, których dane dotyczą, a swobodą zbierania, wykorzystywania i przekazywania informacji.

Swobody informacyjne to zresztą nie tylko sprawa indywidualnych wolności obywatelskich, ale także problem wypełniania przez administrację i odpowiednie instytucje różnych funkcji publicznych. Wytyczając reguły ochrony danych osobowych należy uważać, aby nie przekroczyć granicy, za którą słuszne i szlachetne zamiary oraz założenia zaczynają już wywoływać negatywne skutki: ma to miejsce na przykład wówczas, gdy zbyt rygorystyczne ograniczenia w pozyskiwaniu i gromadzeniu informacji (danych osobowych) przeszkadzają w zapewnieniu porządku i bezpieczeństwa albo nie pozwalają administracji zajmującej się sprawami socjalnymi należycie wykonywać zadania i sprawiedliwe dzielić dobra między potrzebujących. Omawiany problem dostrzegli autorzy Konwencji (nr 108) Rady Europy z 28 I 1981 roku, dotyczącej ochrony osób w związku z automatycznym przetwarzaniem danych osobowych[19]. W jej preambule, zaraz po „przypomnieniu" – jak to sformułowano – prawa do poszanowania prywatności, znajdujemy następujące stwierdzenia: „Potwierdzając jednocześnie [...] zobowiązanie na rzecz swobodnego przepływu informacji bez względu na istniejące granice; Uznając konieczność pogodzenia podstawowych wartości poszanowania prywatności ze swobodnym obiegiem informacji między narodami [...]".

Ustalenie zakresu ochrony danych osobowych w oparciu o nową polską ustawę będzie zapewne, w kontekście funkcjonujących współcześnie sieci komputerowych, źródłem wielu wątpliwości, których rozstrzygnięcie pozostanie ostatecznie zadaniem sądów. Nie jest jednak wykluczone, że ograniczenie obszaru niepewności prawnej osiągnięte zostanie przez wydanie – wzorem Niemiec – dodatkowych, „uzupełniających przepisów", mających na uwadze wprost i wyłącznie możliwości niedozwolonego posługiwania się danymi osobowymi przy świadczeniu różnorakich usług z wykorzystaniem sieci komputerowych. Tak czyni niemiecka Teledienstedatenschutzgesetz, stanowiąca część złożonego, kompleksowego aktu prawnego poświęconego usługom informacyjnym i komunikacyjnym (Informations- und Kommunikationsdienste-Gesetz z 1 sierpnia 1997 roku). Znajdujemy tam postanowienia dotyczące między innymi zasad przetwarzania danych, zobowiązań dostawcy usług w sieciach, swobody umów ze względu na zbieranie danych; wyznaczone zostały również dopuszczalne granice wykorzystywania zarówno danych osobowych, jak i danych informujących o korzystaniu przez określoną osobę z usług w sieciach. Na uwagę zasługują też regulacje, które zakazują praktyk polegających na uzależnianiu umów z dostawcami usług w sieciach od zgody osoby na wykorzystanie

---

[19] Określanej dalej skrótowo jako konwencja z 1981 roku lub konwencja strasburska.

jej danych osobowych do odmiennych celów, o ile nie jest możliwe uzyskanie przez nią takiej usługi w inny sposób.

Co istotne, w omawianej ustawie niemieckiej sformułowana została generalna zasada stwierdzająca, że dane osobowe mogą być zbierane, przetwarzane i wykorzystywane jedynie w zakresie koniecznym, niezbędnym do zawarcia umowy w sprawie usługi oferowanej przez dostawcę oraz do ustalenia lub zmodyfikowania warunków takiej umowy. Wykorzystanie tych danych w celu reklamy, porad, badań rynkowych albo badań dotyczących zapotrzebowania na „usługi sieciowe" wymaga wyraźnej zgody zainteresowanego. Jeżeli chodzi natomiast o dane dotyczące korzystania z „usług sieciowych" przez użytkownika, to mogą być one wykorzystywane wyłącznie w zakresie umożliwiającym realizację usług albo w zakresie koniecznym do ustalenia należnej opłaty z tego tytułu. Dane powyższe nie mogą być udostępniane osobom trzecim, w tym innym dostawcom usług.

Dodajmy, że omawiana ustawa nakazuje usługodawcom kierować się przy dobieraniu i konfigurowaniu sprzętu technicznego tym, aby dane osobowe były zbierane, wykorzystywane lub przetwarzane w możliwie najmniejszym zakresie.

7. Opisując i analizując nowe uregulowania dotyczące ochrony danych osobowych nie sposób pominąć nie całkiem wyjaśnioną kwestię relacji, jakie zachodzą w stosunku do powszechnej ochrony dóbr osobistych (wykonywaną w Polsce przede wszystkim na podstawie przepisów kodeksu cywilnego). W szczególności można rozważać, czy ochrona ustanowiona wymienioną ustawą z 1997 roku stanowi jedynie realizację, ukonkretnienie w zakresie pewnych praktyk społecznych, powszechnej ochrony dóbr osobistych, będąc względem niej swoistym lex specialis, czy też mamy tu do czynienia z autonomicznym obszarem prawnym.

Można przytoczyć szereg argumentów przemawiających za tym, iż specjalne przepisy o ochronie danych osobowych związane są z realizacją powszechnego prawa do prywatności (right to privacy), którego istotą jest eliminowanie ingerencji w życie osobiste, gwarantowanie każdemu człowiekowi tego, że będzie pozostawiony w spokoju, zapewnienie mu możliwości decydowania o ujawnianiu, udostępnianiu i wykorzystywaniu elementów swego szeroko rozumianego wizerunku. Znalazło to odbicie we wspomnianej już konwencji strasburskiej z 1981 roku. W wyjaśniającej jej genezę i funkcję preambule znajdujemy między innymi stwierdzenie: „Zważywszy, że pożądane jest poszerzenie ochrony praw i podstawowych wolności każdego człowieka, w szczególności prawa do poszanowania prywatności [...]". Tę myśl powtarza przepis artykułu pierwszego konwencji, który stwierdza, iż „konwencja ma na celu zagwarantowanie, na terytorium każdej ze stron, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowanie jej praw i podstawowych wol-

ności, w szczególności jej prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych («ochrona danych»)".

Odniesienie do podstawowych praw i wolności, a w szczególności prawa do prywatności, zostało uwidocznione także w dyrektywie Parlamentu Europejskiego i Rady Europy z dnia 24 X 1995 roku (95/46/EG) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych[20]. W jej preambule (w punktach 2. i 10.) czytamy: „Będące na usługach człowieka systemy przetwarzania danych muszą szanować podstawowe prawa i wolności osób, w szczególności ich sferę prywatności, niezależnie od przynależności państwowej i miejsca zamieszkania, przyczyniając się do rozwoju handlu oraz dobrobytu ludzi. [...] Przedmiotem obowiązujących w poszczególnych krajach przepisów dotyczących przetwarzania danych jest zagwarantowanie podstawowych praw i wolności, w szczególności prawa do prywatności przewidzianego w artykule 8. Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Harmonizacja uregulowań nie może zatem prowadzić do ograniczenia zapewnionej przez te przepisy ochrony, lecz przeciwnie, powinna zmierzać do ustanowienia we wspólnocie wysokiego poziomu ochrony".

O szczególnym zbliżeniu ochrony praw osobistych do ochrony danych osobowych można mówić na gruncie prawa niemieckiego. Za sprawą Federalnego Sądu Konstytucyjnego (przez wydanie w 1983 roku głośnego orzeczenia Volkszahlungsurteil) zostało wprowadzone w latach osiemdziesiątych do niemieckiego porządku prawnego tak zwane prawo do informacyjnego samookreślenia się (Recht auf informationelle Selbstbestimmung). Niewątpliwie asumpt do wykreowania takiego prawa, któremu nadano rangę konstytucyjną, dały obawy związane z rozwojem nowych metod zbierania, gromadzenia i przetwarzania informacji o osobach. Uznano za niezbędne zapewnienie każdemu obywatelowi władztwa nad zakresem istniejących na jego temat informacji. Takie podejście nakłada na ustawodawcę obowiązek stworzenia instrumentów, dzięki którym aksjologiczna idea praw zasadniczych, konstytucyjnych, znajdowałaby spełnienie w obrębie prawa prywatnego. Chodzi o uprawnienie pozwalające samodzielnie rozstrzygać, kiedy oraz w jakich granicach ujawniane miałyby być osobiste sytuacje życiowe, i to uprawnienie nie sprowadzone do relacji obywatel – państwo, ale odnoszące się też do wzajemnych stosunków między obywatelami[21].

8. Lektura polskiej ustawy z 1997 roku o ochronie danych osobowych pozwala zauważyć brak odesłań lub nawiązań do prawa do prywatności czy in-

[20] Określanej dalej skrótowo jako: dyrektywa o ochronie danych osobowych. Na jej temat por. m.in.: De Terwangne, Louveaux, dz. cyt., s. 451n.

[21] Por. z nowszych wypowiedzi: B. Sokol, *Datenschutz in der Informationsgesellschaft*, „Multimedia und Recht" 1998, nr 9, s. 7-10.

nych powszechnych dóbr osobistych. Sam brak w jej przepisach wyraźnego odniesienia tego rodzaju nie jest wprawdzie rozstrzygającym i niepodważalnym argumentem na rzecz tezy o „oderwaniu" ustawowej regulacji od powszechnego prawa do prywatności. Taki stan rzeczy sprzeciwia się jednak patrzeniu na tę regulację przez pryzmat prawa do prywatności i nakazuje co najmniej ostrożność, jeśli chodzi o jej „korygowanie" przez zasady wypracowane w literaturze i orzecznictwie odnośnie do powszechnych praw osobistych, w tym prawa do prywatności.

Także Konstytucja RP nie łączy ochrony danych osobowych z prawem do prywatności. Obydwu tym kwestiom poświęca odrębne przepisy (o prawie do prywatności mówi w artykule 47., o danych osobowych w artykule 51.); brzmienie tych postanowień nie upoważnia w żadnej mierze do tego, aby upatrywać istnienia bliskiego związku pomiędzy regulowaną w nich materią. Nie wchodząc w rozważania teoretyczne przekraczające ramy tego artykułu wydaje się, iż można przyjąć, że pomiędzy ochroną prawa do prywatności (występującą na płaszczyźnie prawa konstytucyjnego oraz w ramach powszechnych dóbr osobistych) a ochroną danych osobowych (dostrzeganą w nowej Konstytucji RP, a szczegółowo ujmowaną w omawianej w tej opinii ustawie z 1997 roku) zachodzi stosunek krzyżowania w tym tylko sensie, że istnieją zachowania, którą mogą równolegle naruszać ochronę przewidzianą w obu rozważanych płaszczyznach. Są to przy tym reżimy wzajemnie niezależne. Oznacza to, że w wielu przypadkach nieuprawnione przetwarzanie danych osobowych będzie nosiło znamiona niedozwolonej ingerencji w prawo do prywatności; także ochrona prawa do prywatności będzie polegać nierzadko na sprzeciwianiu się wykorzystywaniu przez osoby trzecie cudzych danych osobowych. Obok tego jednak wystąpić mogą również sytuacje, w których przetwarzanie danych zapewne nie zostałoby zakwalifikowane jako naruszenie prawa do prywatności[22]; podobnie można wyobrazić sobie przypadki wkroczenia w objętą ochroną sferę prywatności poprzez działania inne niż przetwarzanie danych osobowych. W konsekwencji dochodzenie ochrony w oparciu o przepisy omawianej ustawy z 1997 roku nie będzie wymagało wykazania, iż doszło do naruszenia prywatności, przynajmniej tak jak jest ona rozumiana w kontekście ochrony dóbr osobistych na gruncie kodeksu cywilnego.

---

[22] Zauważmy, iż w istniejącym stanie prawnym charakter danych osobowych posiadają informacje „z różnych dziedzin życia", o ile tylko istnieje możliwość powiązania ich z oznaczoną osobą. Mogą to być informacje dotyczące samej osoby (jej pochodzenia, miejsca i daty urodzenia, rodziców, cech fizycznych, wyglądu, jak również „przynależnych jej" dokumentów tożsamości), jej cech intelektualnych (poglądów, przekonań, wykształcenia, zdobytych kwalifikacji), sytuacji rodzinnej, przygotowania zawodowego i przebiegu pracy, stanu majątkowego i dokonywanych operacji finansowych, jej zachowań (podróży, zakupów towarów lub usług, naruszeń prawa) itd. Do rzędu danych osobowych zaliczyć należy między innymi informacje o tym, czyim klientem jest określona osoba, z kim wiąże ją stosunek prawny o charakterze ciągłym. Dane tego rodzaju, jak widać, są niezależne od takich kryteriów jak intymność.

Jeśli przetwarzanie danych osobowych stanowi równocześnie bezprawne naruszenie prawa do prywatności, będziemy mieli do czynienia z ochroną kumulowaną. Jest to sytuacja przewidziana przez kodeks cywilny w tym sensie, że przepis artykułu 23. kodeksu cywilnego wyraźnie zastrzega, iż dobra osobiste człowieka (do których powszechnie zalicza się też prywatność) „pozostają pod ochroną prawa cywilnego, niezależnie od ochrony przewidzianej w innych przepisach". Do rzędu tych „innych przepisów" można zaliczyć także przepisy ustawy z 1997 roku o ochronie danych osobowych.

Okoliczność, iż w danym przypadku „zbiega się" ochrona wynikająca z przepisów kodeksu cywilnego oraz z ustawy z 1997 roku, nie powinna bynajmniej powodować, że dochodząc ochrony na podstawie tej ustawy należy brać pod uwagę przyjęte w prawie cywilnym:

a) przesłanki ochrony statuowane w prawie cywilnym,

b) okoliczności uchylające bezprawność działania.

Dodajmy, że w istocie przewidziane w ustawie okoliczności usprawiedliwiające przetwarzanie danych osobowych pokrywają się w znacznej mierze z kryteriami egzoneracyjnymi stosowanymi na gruncie prawa cywilnego odnośnie do ochrony powszechnych dóbr osobistych. Mamy tu na myśli nie tylko zgodę zainteresowanego, ale też działanie w jego interesie, działanie w ramach przepisów prawa, wykonywanie określonych prawem zadań realizowanych dla dobra publicznego (por. art. 23 u.o.d.o.). Natomiast autonomiczność regulacji zamieszczonej w omawianej ustawie w stosunku do norm prawa cywilnego znajduje wyraz w tym, że przesłanki dopuszczalności przetwarzania danych osobowych ujęte są odmiennie, i co istotniejsze – szerzej niż przesłanki uchylające bezprawność ingerencji w dobra osobiste, o których mowa w artykule 23. kodeksu cywilnego.

Teoretycznie można by jeszcze stosunek między przepisami o ochronie prywatności i przepisami o ochronie danych osobowych ująć w relację lex generalis – lex specialis. Dla takiego stanowiska trudno jednak znaleźć oparcie w brzmieniu czy systematyce przepisów. Zastrzeżenia wzbudzałyby także konsekwencje takiego ujęcia polegające między innymi na ograniczeniu zakresu stosowania ochrony opartej na przepisach artykułów 23. i 24. kodeksu cywilnego. Tymczasem w orzecznictwie Sądu Najwyższego daje się zauważyć raczej tendencję do rozszerzającego interpretowania zakresu ochrony wynikającą ze wspomnianych przepisów. Mimo że w katalogu chronionych dóbr nie wymieniają one expressis verbis prywatności, to Sąd Najwyższy nie miał wątpliwości, iż: „otwarty katalog dóbr osobistych (artykułów 23. i 24. kodeksu cywilnego) pozwala na włączenie do ich zakresu dóbr, które są związane ze sferą życia prywatnego, rodzinnego, ze sferą intymności"[23].

[23] Orzeczenie Sądu Najwyższego z 18 I 1984 r., opublikowane w: „Orzeczenia Sądu Najwyższego" 1984, z. 11, poz. 195.

9. Powyższe skrótowe uwagi zaledwie sygnalizują niektóre zagadnienia dotyczące ochrony prywatności w społeczeństwie informatycznym. Jak łatwo jednak dostrzec, pojawiają się wcześniej nie znane rodzaje zagrożeń, czemu towarzyszy poszukiwanie nowych, adekwatnych regulacji prawnych. Zmienia się też częściowo samo rozumienie i podejście do kwestii prywatności[24]. Zaciera się granica pomiędzy tradycyjnie rozumianą ochroną prywatności a ochroną danych osobowych. Cechy „prywatności" nabywają dzisiaj, zwłaszcza wobec możliwości, jakie przyniosła ze sobą nowoczesna technika informatyczna, właściwie wszelkie już dane (informacje) dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby [25]. Taką właśnie definicją posługuje się dyrektywa Unii o ochronie danych osobowych[26]. Charakter danych tego rodzaju posiadają informacje „z różnych dziedzin życia", o ile tylko istnieje możliwość powiązania ich z oznaczoną osobą[27].

Ten stan stawia przed prawnikami nowe problemy i pytania: Jak dziś rozumieć prawo do prywatności? Na ile można stworzyć ogólną, syntetyczną definicję obejmującą swym zakresem wszystkie zasługujące na ochronę, w kontekście nowych sytuacji faktycznych, interesy jednostki? Z poszukiwaniem odpowiedzi na to pytanie związane są poważne konsekwencje praktyczne, w tym także na płaszczyźnie prawa międzynarodowego. Bo przecież od tego, jakie znaczenie nadamy pojęciu „prywatność", „życie prywatne", zależeć będzie w znacznej mierze zakres działania przywołanego na wstępie artykułu 8. Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności przepisu, który mimo postępu prawa i zmian stosunków społecznych, w niczym nie stracił na znaczeniu. Bo też nie straciła na znaczeniu idea – o której pisał A. Kopff – „życia własnym życiem, układanym według własnej woli, z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej"[28].

---

[24] Prawo do prywatności już teraz bywa niejednokrotnie definiowane w sposób – można tak powiedzieć – informatyczny, jako prawo decydowania oraz kontrolowania pozyskiwania i obiegu określonych informacji (zasadniczo informacji o sprawach osobistych, rodzinnych).

[25] Kwestionowana bywa kategoria „danych wolnych", których zbieranie i wykorzystywanie byłoby prawnie nieistotne. Uważa się, iż zagrożeniem dla słusznych interesów jednostki, zwłaszcza w obliczu obecnej techniki informatycznej, okazać się może przetwarzanie nawet takich danych, jak imię, nazwisko, wiek czy miejsce zamieszkania.

[26] Podobnie konwencja strasburgska, która stwierdza, iż wyrażenie „dane osobowe" oznacza „wszelką informację dotyczącą osoby fizycznej o ustalonej tożsamości albo dającej się zidentyfikować".

[27] Do rzędu danych osobowych wymienionych w przypisie 22 zaliczyć należy m.in. informacje o tym, czyim klientem jest określona osoba, z kim wiąże ją stosunek prawny o charakterze ciągłym. Zauważmy nadto, iż nie są a limine wyłączane z zakresu ochrony „dane jawne" dostępne innym osobom.

[28] K o p f f, dz. cyt., s. 30.